Prevention of Future Cybercrime
A Proactive Approach for Better Future

Masud Parvez Chowdhury[1]

[1]Bangladesh Army
masud696@gmail.com

Abstract. A recent study shows that the crime trend is shifting towards cyber space. People who are not aware of the current trend of cybercrime are being victimized. The study has been carried out to identify the current trend of crime happening in the cyber space with a view to figuring out proactive defense mechanism against it. The study indicates that the cyber criminals are exploiting the vulnerabilities of the internet users and attacking them with ill motives. A time worthy proactive approach to mitigate cybercrime is likely to benefit internet users to safeguard themselves in the cyber space. Internet is directly connected to cybercrime which is in a sharp rise in the current world. Cybercrime is increasing day by day because of global connectivity and its rapid escalation. Since the future technology is Internet of Things (IoT) so the future crime is anticipated to be biased towards that. More connectivity will definitely make people more vulnerable to cybercrime. However, that should not keep them away from connectivity but proper safety measures should be taken. Since the lack of knowledge regarding cybercrime and absence of awareness seems to be the prime reason for people being victimized of cybercrime so enlightening them with adequate knowledge against cybercrime is likely to enhance cyber security

Keywords: Changing Trend of Crime, Future Cybercrime, Prediction, Proactive Approach.

1 Introduction

Crime is nothing new in this world. It started from the beginning of marking. But cybercrime is a new dimension in the crime scenario. Cybercrime around the world started in recent past which is very dynamic in nature. The cyber criminals are always finding new techniques to deceive and bluff their targets. The way the world is moving towards technology, the similar way the crime is changing its dimension and moving towards cybercrime. This cybercrime is changing its pattern with the changing scenario of technology [1].

The world is highly benefitted by technology but at the same time it has put people at a high risk of crime which is done with the use of technology. Slowly and gradually people are moving towards a world where every single task will be done through technology and every single device will be connected [2-4]. So, the future cybercrime will open new dimensions where the criminals are likely to use sophisticated technology and dynamic techniques to avoid detection. Future criminals will always try to remain one step ahead with the use of latest technology where the detective agencies leg behind. Taking counter measures against cybercrime is not only the responsibility of the government agencies but also every individual. As a result, all the government agencies and every individual must have adequate knowledge on current and future cybercrime to arrest it [5-8]. This paper aims to analyze the trend of crime from past to future, the factors affecting the future cybercrime, the significance and rapid move of technology in human life and the dark side of technological advancement in the society. It also suggests methods to prevent future cybercrime through knowledge, wisdom and technology with a view to making a better future.

2 Background of the Study and Related Work

Cybercrime is happening everyday around the world and the graph is alarmingly going high. Number of reports and survey shows that crime is switching from physical to digital [9,10]. Currently people are living in a world where they cannot refrain themselves from the use of technology. Even the people who are living in remote villages are using technology every day in many occasions. People cannot but have to use technology to make phone calls, to use over the top applications, to communicate with relatives and friends who are living abroad, to use social media and many more [11-14]. Although technological advancement is proving huge benefit to the people but at the same time it is making them vulnerable to cybercrime.

3 Methodology

3.1 Data Collection

The paper has been articulated basing on different data. Relevant data was collected on contemporary cybercrime issues with a view to figuring out a predictive scenario for future cybercrime. The data has been collected from different libraries, online open-source materials and survey results. The collection of data was focused on the state of current cybercrime, different types of cybercrime in the current world, reasons for current cybercrime etc The collection procedure will include two phases. In first phase, researcher will collect data from open-source materials and in the second phase collect data through different survey.

3.2 Data processing

After collection of various data, it was processed to extract relevant information pertaining to cybercrime in current world. In this phase different types of data mining techniques were adopted to get desired results. Different open and free version data mining software were used for data mining form the data warehouse.

3.3 Data Analysis

To understand the pattern of cybercrime, the qualitative and descriptive mechanism is the most ideal means of collecting and analyzing data due to its flexibility and addictiveness and immediacy of the topic. In this paper the processed data was analyzed for better understanding of current cybercrime and to anticipate future cybercrime to figure out defensive measures.

3.4 Evaluation

After analysis of the processed data, it was evaluated to determine whether it is suitable for drawing deductions and useful for recommendations or not. The evaluated data has been used to carry out research work to come to a plausible assumption about the best approach to curve cybercrime for better future.

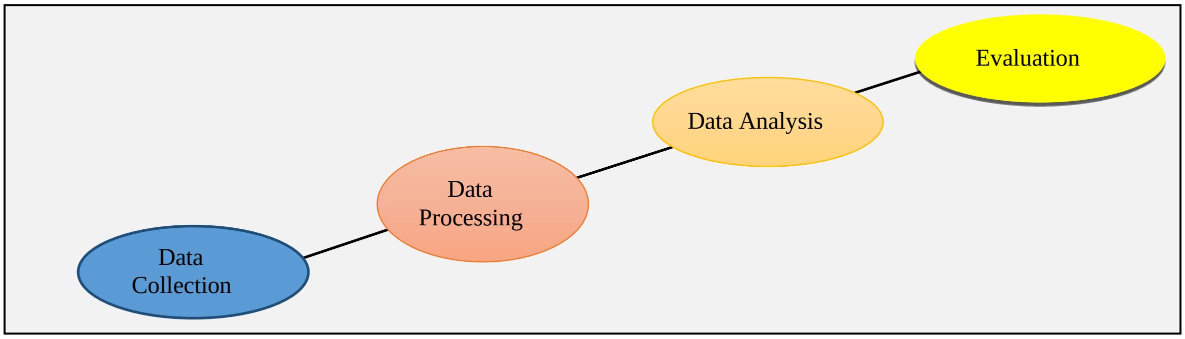

Fig. 1. Proposed Workflow

4 Paradigm Shift of Crime

4.1 The Changing Trend of Crime

Criminals exist in the society from the beginning of mankind. But they change their behavior, techniques and trend of crimes. Most of the crimes since inception are caused by poverty or other forms of social deprivation. But the analysis of history of crime shows that physical crimes like murder, violent crime and crime with knife is decreasing day by day. On the other hand, there is a sharp rise in social crime which is done through internet and smart devices. We have entered an era of incredible technological innovation. The increased activities of hackers, scammers and other online criminals had changed the trend of crime. Below is discussed some incidents that will highlight the changing trend of crime.

2007, a case of child abuse. A plumber entered into the house of a child in absence of her parents. He entered with a plea of working with bathroom fittings. Before this, he carried out reconnaissance of the house and made a master plan to fulfill his evil desire. On that day, in absence of her parents, the plumber started molesting her. But fortunately, her parents came back to the house at that moment and the plumber was caught red handed. Getting this news, security personnel rushed to that house and heard the story from everyone (four of them). The plumber was asked that why did he go to that house. He replied that he went to repair a tap which was leaking and showed a tap tied with rope. Then the plumber was asked to untie the rope and tie again. The plumber could not tie it the way it was tied before. Then the father of the girl was asked to tie it and he did it exactly it was done before. So, it was understood that the plumber lied and finally he confessed everything. So here we can see that the crime and detection both were physical.

2009, a case of suicide for extra marital affair. The person who committed suicide was serving in Tangail district. He developed extra marital affair with a lady who was from Rajshahi district. One day that person went to Rajshahi, murdered that lady and came back to Tangail silently and undetected. When the murder spot was investigated, the investigation team came to know that two mobile phones of the victim were missing. The investigation team took it as a lead to detect the murderer. The person who murdered was may be a cool-headed killer who came back from the spot undetected and continued doing all his routine jobs. But technically he was not sound and that brought him to the breaking point. He brought the mobile phones of the lady and deleted all evidences between them. He formatted the mobile phone, thrown away the SIM cards and started using the phones with new SIM cards. He did not know that, everything inside the mobile handset can be deleted, SIM card can be changed but the IMEI number is unique and unchangeable. Ultimately with the help of the IMEI number, detectives reached him. When the person was detected, he committed suicide. Here the crime was physical but detection was digital.

2016, A case of bank robbery amounting 80 million USD from Bangladesh Bank through digital technology. As per the report of the investigating committee, the swift system was connected to Real Time Gross Settlement (RTGS) which created the vulnerability. This caused the network vulnerable and the swift system became insecure. Exploiting this vulnerability, the hackers stole the swift code and shifted 80 million USD to their accounts without any physical involvement. Here the crime was completely digital and detection is still incomplete due to inferior technology.

2017, another case of suicide, this time it was a lady and crime detection was digital. Nowadays social media, specially Facebook is very popular in Bangladesh. Like many others, the lady got addicted to Facebook. In course of time, she got number of Facebook friends and developed intimacy with three men. Her intimate friends started alluring her for growing more intimacy and moving towards physical contact. At one stage, she stepped into the trap and started fulfilling her Facebook friends' evil desires. Even she allowed them to take intimate pictures with them and recording videos of physical contact. All her friends who grew illicit relation with her were married but did hide the fact. She started dreaming to marry one of them with no knowledge about his background. Ultimately her all three Facebook friends came to know her relation with each of them. One of the friends started threatening and blackmailing her for having relation with others. Subsequently all these stories and quarrels travelled to her parents, friends and family members. Finally, she had no other way but to commit suicide. After her death, all the crimes and criminals were detected through digital footprint. So here both the crime and detection were done with the help of technology.

2019, number of cases were detected for identity and password theft. The hackers were using this technique to blackmail the Facebook users. The hackers use spyware and key logger for identity and password theft and subsequently take over full control of other’s Facebook ID. After doing so, they establish contact with different friends of that ID and look for gain. The hackers also upload pornography from the hacked IDs and try to blackmail the owner of the IDs. Here the crime is highly technical and detection is still very difficult.

2021, fear of spyware into the electronic devices prevailing everywhere. The spyware if intruded inside the devices can steal all the data inside that device. Most of the spyware use phishing link and fool the users by alluring content to click it and device get compromised. But very recent development has brought out subzero click spyware which even does not need user’s notification or any click. One such recent spyware is "Pegasus" that can harvest data, turn on mic and camera of a smartphone without the user's input, track location and record keystrokes. So, it can be understood how crime is moving towards technology. That projects a picture of future crime which would be solely technology biased. The technology users won’t even be able to know that his device has been compromised and all data being stolen.

4.2 State of Current Cybercrime

There are number of hacking techniques that the hackers are currently following. The techniques depend on what they want to hack. The hackers generally use social engineering technique followed by phishing. If the users are not careful in their cyber life, then the hackers may also use eavesdropping or key logger to steal password. To slow down any website or blog, the hackers may use Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack technique. Their intension is to earn money, blackmailing, abusing, harassing, taking revenge etc. According to the Cyber Security and Crime Division Department of Dhaka Metropolitan Police (DMP), 70% of cybercrime victims are women, of which 57% are between 18 and 25 years of age. Some 13% of the victims are below 18. The unit gave the findings after analyzing 666 cases and complaints over cyber-related offences filed with different police stations in Dhaka since 2016. The number of such victims had been increasing. The criminals spread defamatory and fake information online using fake IDs and photos of the victims. The offenders also blackmail women after hacking their social media profiles. Approximately 1% of the 666 cases were related to terrorism, 7% to blackmail or extortion, 14% to pornography, 14% to financial frauds, 20% to hacking, 18% to deflation, 20% to fake IDs and 6% other issues. Figure 2 shows the types of current cybercrime.

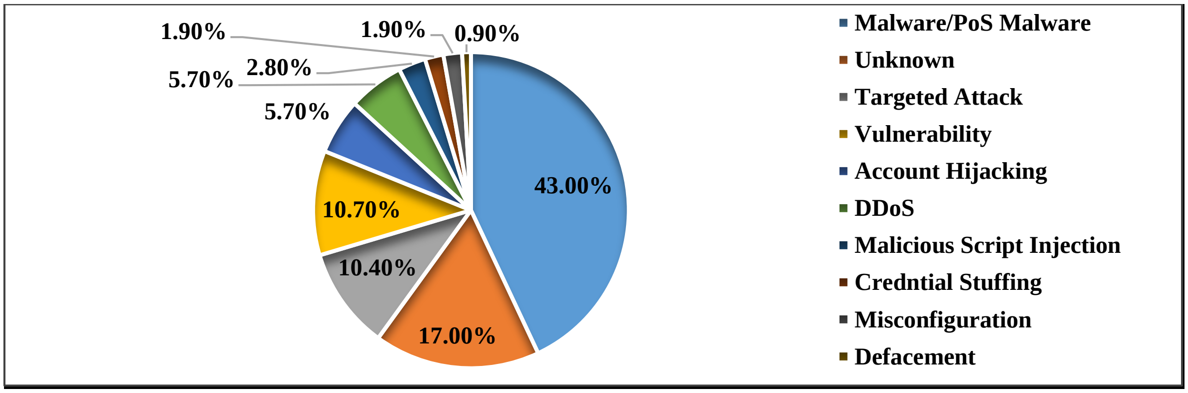

Fig. 2. Types of Current Cybercrime. Source: DMP Crime Division Report

4.3 Nature of Current Cybercrime

- **Crime against Person and Property**

Most of the current cybercrimes are committed against individual and property. Major targets are individuals and prime reason for targeting individual is personal gain. There are various types of cybercrimes against persons and property such as cyber bulling, identity and password theft and subsequently blackmailing and seeking financial gain.

- **Crime against Institution/ Organization**

There are several cybercrimes happening every day against different institution/ organization within government or private sectors. This is specially done for defaming an institution, business interest or unhealthy race amongst institutions.

- **Crime against Government**

Cybercrime against government is done at national or international level. There are many vested groups in a country who do cybercrimes against the government to defame them. Specially the opposition parties always try to spread rumor, propaganda against the government to fulfil their desire. At present context, social media is the easiest and largest platform to do this kind of crime.

4.4 Reasons for Current Cybercrime

- **Easy Access to Internet**.

As per the statistics of Bangladesh Telecommunication Regulatory Commission (BTRC) and Internet Service Provider Association of Bangladesh (ISPAB) 81.7 million people of Bangladesh are using internet.

People are getting 24 hours access to internet through their smartphones. That is one of the prime reasons for current cybercrimes and also victimization [15, 16]. Figure 3 shows the increasing number of internet users in the world and figure 4 demonstrates the state of technology used in Bangladesh.

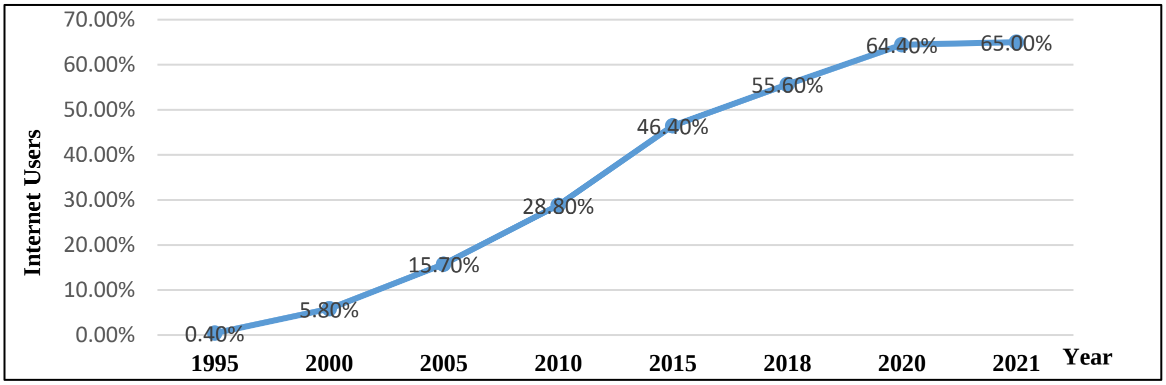

Fig. 3. Number of Internet Users around the World. Source: Global Report

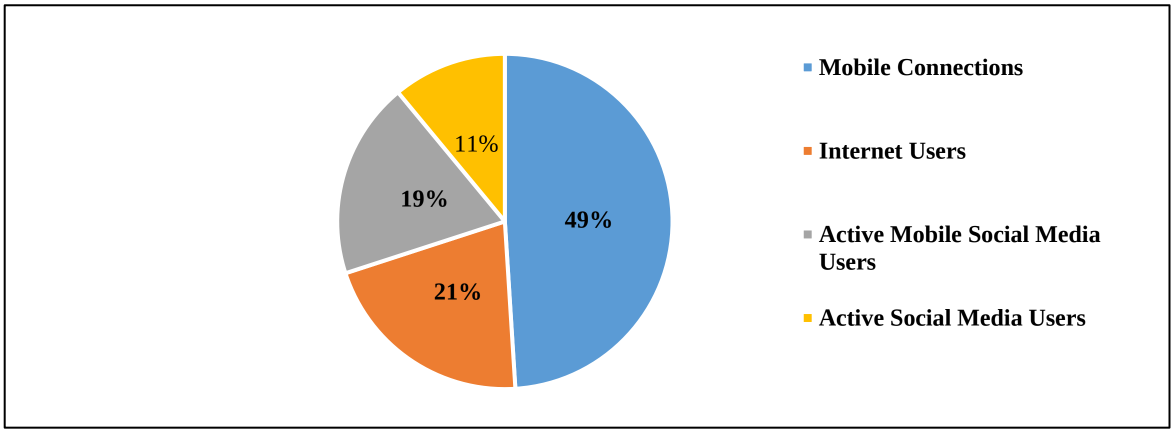

Fig. 4. State of Digital Bangladesh (Use of Technology). Source: BTRC

- **Addiction to Social Media**

The current generation are highly addicted to social media, specially Facebook. They love to earn name and fame through the social media. The more like, share and comments they get in their pictures and status the happier they feel [17, 18]. Many of them start dreaming themselves as celebrity as they become popular on Facebook. To increase the number of likes, shares and comments, they develop friendship with unknown person and subsequently fall into trap. This is how the hackers trap them and blackmail them. The hackers follow the technique of social engineering to get closer to their target and gather information about him/ her. Gradually they grow intimacy and finally drag them into the trap to fulfill their evil desire. Figure 5 shows the statistics of uses of social media in Bangladesh.

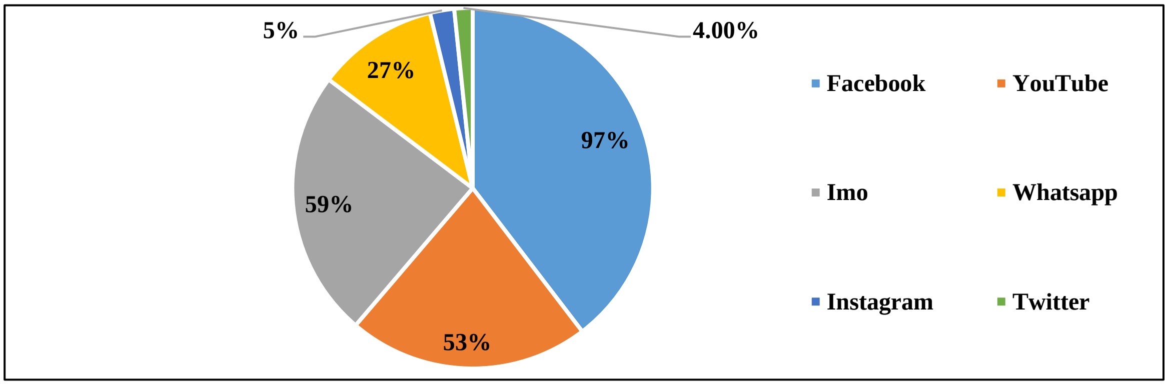

Fig. 5. Social Media Statistic in Bangladesh. Source: Internet

- **Addiction to Porn Sites**

A person who is 24 hours connected to the internet, tend to be allured by the porn sites. Whenever someone is surfing through his Facebook or any other website, he is likely to come across some alluring content. These alluring contents drag him to porn sites. Thus, the youth and even the aged people become addicted to porn sites.

- **Religious Demotivation**

There are tens of thousands of religious contents available in the internet. Some of these are true, some are fake. Evil minded people spread fake religious content to demotivate people. Those who do not read Quran and Hadith, depend on the net content which are not fully authentic. Thus, they fall into the trap of wrong doers and get demotivated. This is how religious extremism is spreading in the society.

- **Financial Gain**

The hackers mainly do cybercrime for financial gain. They with their hacking knowledge do the identity and password theft of different social media IDs of general people and blackmail them for financial gain.

- **Lack of Knowledge and Awareness**

Many of us do not know what is Cybercrime and how it is done. Many do not know that digital footprint of the hackers can back track them to identify thefts cases and digital thieves. Due to this lack of awareness and technical knowledge they fall into the trap of the hackers [19, 20].

5 Prediction of Future Cybercrime

Greater connections invite greater risks. A medical device like pacemakers can be hacked to deliver a lethal weapon of electricity and a car's brake can be disabled at high speed from miles away. A 3D printer can produce AK-47 and fleets of drones may be used to ferry drugs across borders. Future cybercrimes explore how bad actors can hijack the technologies of tomorrow through artificial intelligence. Most of the crime then were through sharp edged weapons. But now and in future would be trough technology. The scenario of cybercrime has changed dramatically with the popularity of smart devices. This is where the fear of future crime indicates. Figure 6 shows the distribution of targets and figure 7 shows the motivation behind attacks.

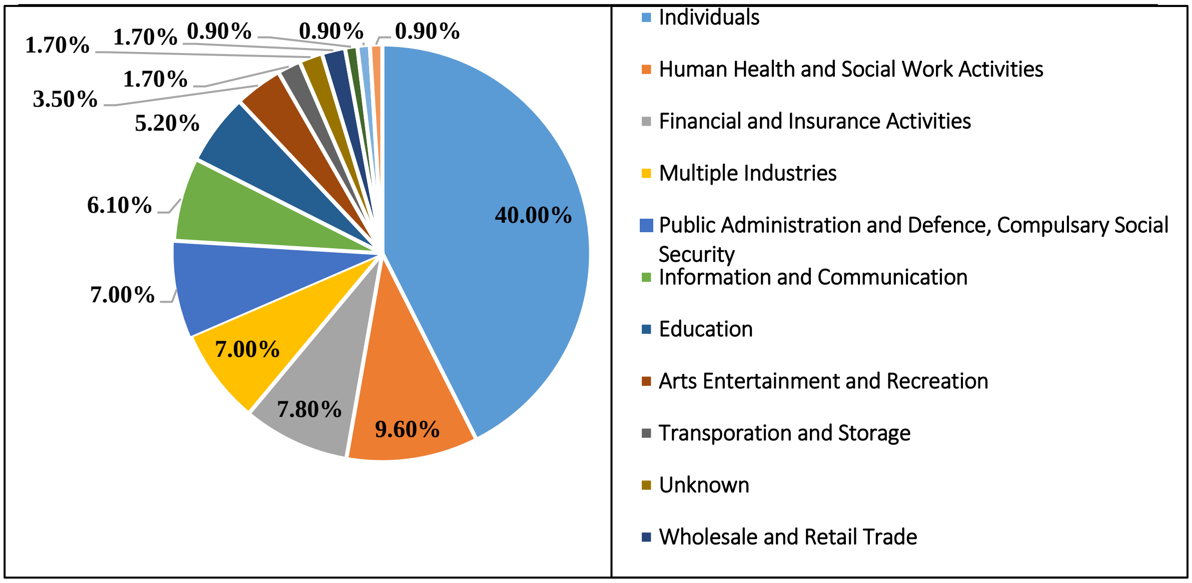

Fig. 6. Distribution of Targets. Source: Survey Results

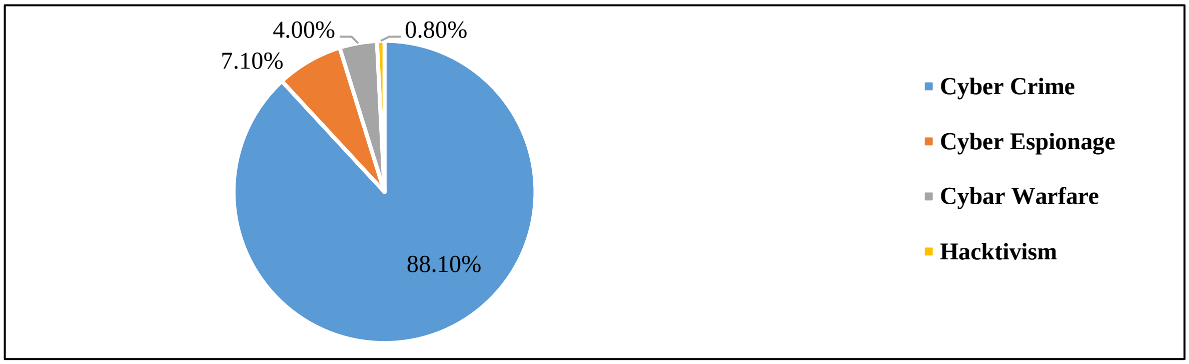

Fig. 7. Motivations behind Attacks. Source: Survey Results

5.1 Future Cybercrime - Technology – Nexus

In future the young offender will commit complex electronic and computer-based crimes, such as stealing electronic signals, hacking into computer networks for the purpose of vandalism and profit. As far as the future victims of cybercrime are concerned, individual, organizations and government will continue to be victimized by a wide range of organized and unorganized electronic and intellectual crime. The general public will continue to be principal target of property crime specially as long as the consumer of electronic products continue to grow.

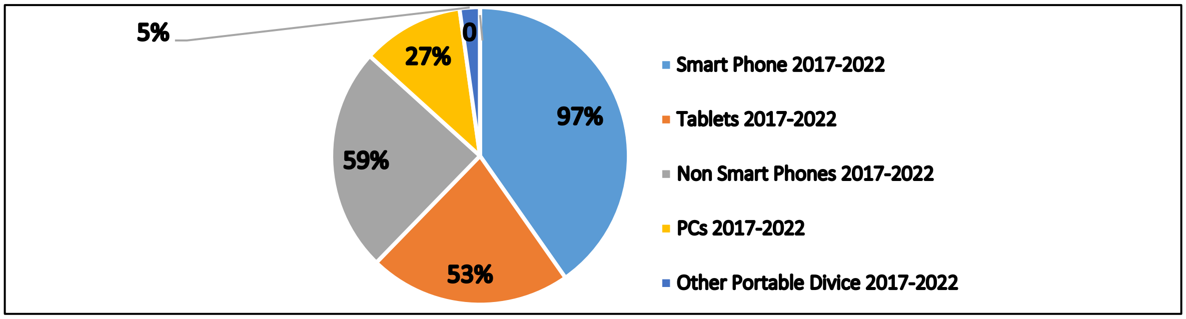

Fig. 8. Increasing Trend of Smartphone Usage. Source**:** Survey Result

The greatest crime threats to organizations may come from attempts to steal information and knowledge. The graphs below show how faster the use of technology and speed of internet is increasing globally. Survey found a rapid decline of non-smartphone from 34 percent in 2017 to 10 percent by 2022 and growth of smartphones from 50 percent in 2017 to over 65 percent by 2022. The most noticeable growth is going to occur in machine-to machine connections. Figure 8 illustrates the increasing trend of smartphone and figure 9 shows the increasing trend of internet speed in GBPS.

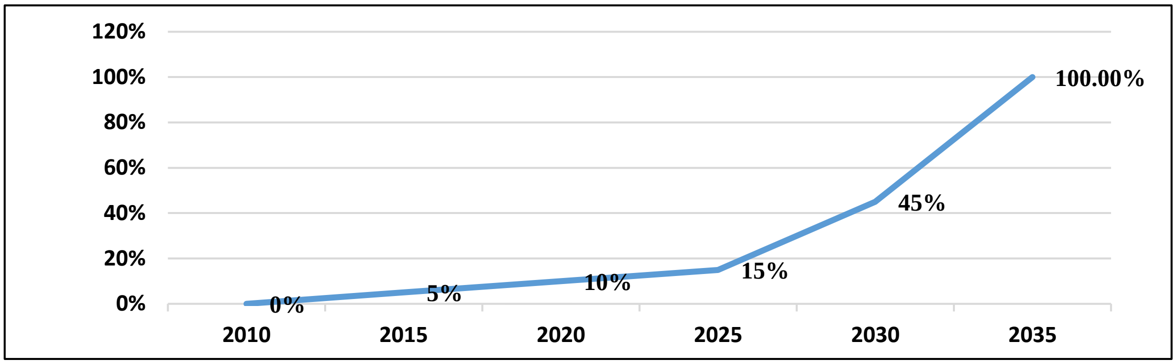

Fig. 9. Increasing Trend of Internet Speed in GBP. Source: Internet

6 Prevention of Future Cybercrime

6.1 Individual Approach

On 07 November 2016 at Nasirnagar of Brahmanbaria district, a person named Faruk Mia (fake name Rasaraj Das) was accused of posting an objectionable image of Holy Kabah from his Facebook. It was later found that his Facebook was used by someone else. Actually, he went to an internet café, browsed his Facebook and left the cafe without logging out his Facebook ID. Someone took the chance and posted the image from his Facebook and Faruk was caught. Later on, after lot of investigation, the truth surfaced. But his suffering was lot.

On 19 October 2019 a Facebook post became viral. It was later known that a student of BholaGovt College named Biplob Chandra Shuvo who's Facebook ID was hacked and anti-Islamic post was shared from his Facebook ID. This created huge chaos and confusion across the country. As a result, general mass confronted police and four people died on the spot by gun shot. So, people must be careful about use of social media and ensure maximum security. Following are some suggested individual approach to guard against digital fraud and be aware of future cybercrime:

- **Secure Mobile Devices**

All mobile devices should have layers of cyber security protocols so that even if it lost or stolen, others cannot take over the control of the device, the network IDs and applications. Use of two or multi factor authentication can mitigate threats of being affected by cybercrimes.

- **What to do in Case of Mobile Theft**

Immediately change the passwords of all social media network IDs, email addresses, inform mobile network operators to block the SIM, inform bank account and credit cards to stop all transactions and inform Law Enforcing Agencies about the incident.

- **Protect Your Data and Store Offline**

In every electronic device, people keep large amount of data. It may be secret or confidential files, images, audio or video clips etc. So long it is kept in an electronic device which is connected to the Internet, it is vulnerable. So, it is better to keep all these in a separate portable device which is offline and completely away from internet.

- **Teach Children and Under Command about the Internet Usage**

Children and under commands must be taught about acceptable use of the internet without completely shutting down communication. Make sure they know that they can come to you if they are experiencing any kind of online harassment, stalking or bullying.

- **Upgrade Digital Devices**

Often, it is seen that electronic devices ask for update. It is necessary to updated the devices but people must know and understand what update it is asking for. People should not trust anything at the first instance. This is also a technique followed by the hackers to send the users with a link of update and thereby hack the device.

- **Factory Reset Device in Case of any Doubt**

Spyware like Pegasus once installed in any device will be very difficult to detect and remove. Because it is one of the latest and very strong spywares. There are number of free spyware available in the internet that the hackers can little modify it and use it to hack devices. In this situation one should get backup of all his data or transfer to any portable hard disc and make the factory reset of the device that will erase everything including the spyware.

- **Consult with Experts**

If there is any doubt that the device might have been compromised or hacked, one must consult with any reliable and trustworthy expert. Do not keep the problem and thereby fall into bigger trouble. As per prediction of the future cybercrime, one cannot easily trust anyone when it is a question of electronic device.

6.2 Institutional/ Organizational Approach

- **Ensure People Know the Future Cyber Threats**

Technology is changing every day. To defend from current and future cybercrime people must keep themselves acquainted with the changing technology. The recent spyware “Pegasus” is able to hack the calls and data inside smart devices. It just gives a missed call in WhatsApp from a number that looks like +46737897045 and the job is done. After the missed call, it intrudes inside the victims’ device and gets all the data. Phishing is a hacking technique where the hackers send a link to the target device. If the link is clicked, the device will be completely compromised and hacker will be able to steal all the data. So, if someone does not know about the spyware, he/she is likely to step into the trap. So, to defend hackers, one must know the technology and hackers’ techniques to keep updated and safe.

- **Institutional Technological Development**

Technological competence is a professional development requirement for any organization. In addition, it is now an essential duty for every member of an organization to understand the technology, methods of maintaining safer cyberspace and know how to use it.

- **Capacity Building to Arrest Future Cybercrime**

Any organization should always be one step ahead of the cybercriminals. The criminals should not be able to outsmart any organizations rather be surprised of being detected by higher technology possessed by organizations. It should build such capacity that will be able to predict future cybercrime and guard against the criminals before they are able do any crime.

- **Investment in Cyber Technology for Prediction and Prevention of Future Cybercrime**

Investment in cyber technology had never gone in vain. Generally, people remain one step behind the criminals where as it should have been reverse. The Law Enforcement Agencies should rather be one step ahead of cyber criminals and provide proactive intelligence. So, it is very time demanding that the organizations should have better technology to predict future cybercrime, provide timely information and don’t give criminals any scope of doing crime. Intrusion detection system, intrusion prevention system and layered information security system like Defense in Depth can be implemented in organizational level.

- **Know the Hacker's Trend and Intension**

There are number of hacking techniques that the hacker may follow. The techniques depend on what they want to hack. For hacking any smart device, email or social media, the hackers generally use spyware and the technique they follow is social engineering followed by phishing. If the users are not careful, the hackers may use eavesdropping or key logger to steal password. To slow down any website or blog, the hackers may use DoS or DDoS attack technique. Their intension may be for earning money, blackmailing, abusing, harassing, taking revenge etc. So knowledge on all these will help any organization to have offensive defensive posture.

- **Restrict Access to the Office Network**

It needs to be well thought who actually need access to the office network. In an office network, the list will only include authorized employees and IT personnel. Keeping a watchful eye on current phishing scams, limiting access to sensitive data and password-protecting network equipment helps keep out the people who don’t belong to. User authentication, authorization and accounting should be maintained for network-based services. Encrypted network can be a safer alternative than maintaining an untrusted and open network.

- **Implement Modern Cyber Security Infrastructure**

Modern cyber security infrastructure must be considered prior to implement any internet-based services by assessing vulnerability and penetration testing. Routine auditing is one of the best practices for ensuring cyber security. ‘Single Sign On (SSO)’can be a better alternative for maintaining security of organization services in cyberspace. ‘Secured Socket Layer (SSL)’ and ‘Transport Layer Security (TSL)’ should be ensured for web-based services of any organization to prevent web crawling of the content from any sort of adversary or hacking attempts.

7 Conclusion

Technology has transformed human lives by increasing their quality of living. It made life faster, dynamic and more comfortable bringing people closer to each other in different ways. Now people lives would be very difficult without technology. Internet, communication and technological advancement are pre-requisites for a country’s development. But one the other side of this technology, there is fear of cybercrime, hacktivism, digital fraudulent, blackmail, account hijacking and many more. It is true that people cannot live a single day without technology but at the same time they cannot avoid the threat of cybercrime. So, it is required to strike a balance between use of technology and maintaining cyber security. It is not possible to completely eliminate cybercrime from the cyberspace. No endeavor has succeeded in totally eliminating crime from the globe. The only possible steps are to make people aware of secure use of technology to combat future cybercrime. Rather than recommending any specific technology or any specific product or process, an effort has been taken to outline a framework, parameters and conditions for better future. Skill development and superior technology can empower the population to have the knowledge to be able to anticipate future cybercrime and guard against accordingly. Every individual, organizations and the government need to embark in this journey of prevention and unleash the future cybercrime.

References

1. Marc Goodman, Future Crime, Anchor Publishers reprint edition January 2016.
2. Peter Hitchens, A Brief History of Crime, Atlantic Book Publishers, 10 April 2003.
3. Rajarshi Rai Choudhury, SomnathBasak, DigbijayGuha, Cyber Crimes - Challenges and Solutions, International Journal of Computer Science and Information Technology (IJCSIT) Volume 4(5) 2013.
4. Alice Decker, The Future of Cyber Crime – Challenges and Solutions, CoE, 10 March 2009.
5. Baldwin John, Thrill and Adventure Seeking and the Age Distribution of Crime, American Journal of Sociology 90(6):1326–29, 1985.
6. Dr Linda Elder and Dr Richard Paul, Analytic Thinking, Foundation for Critical Thinking Process, 2010.
7. Richards J Heuer, Jr Psychology of Intelligence Analysis, Centre for the Study of Intelligence, Central Intelligence Agency 1993.
8. Micheal D Bayer, The Blue Planet, National Defence Intelligence College, February 2010.
9. HSARPA, Cyber Security Workforce Handbook, Journals Department of Homeland Security Cyber Security Division, October 2014.
10. K. N. M. Dr Mir Mohammad Azad and S. S. Sharmin, Cybercrime problem areas, legal areas cybercrime law, July2017.
11. H. Shang, R. Jiang, A. Li, and W. Wang, A framework to construct knowledge base for cyber security, IEEE Second International Conference on Data Science in Cyberspace (DSC), June 2017
12. The Crowdstonk Intelligence Team, Global Threat Report 2015.
13. Cyber security market report, https://investingnews.com/daily/tech-investing/cybersecurity-investing.
14. https://en.wikiquote.org/wiki/Wernher_von_Braun.
15. https://www.acs.org.uk/research/crime-report-2019.
16. https://www.europol.europa.eu/publications-documents/cyber-telecom-crime-report-2019.
17. https://archive.dhakatribune.com/business/banks/2020/06/03/bb-files-new-case-overreserve-heist.
18. https://www.prothomalo.com/technology/article/1622060/date.
19. https://op.europa.eu/webpub/com/general-report-2020/en/.
20. https://cyberfutures2025.org.